PNNL 020372

PCT / IB 03 / 01668

04.06.03 WO

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02009651.7

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02009651.7
Demande no:

Anmeldetag:
Date of filing: 26.04.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Security modules for conditional access with restrictions

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F/

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

Security modules for conditional access with restrictions

INTRODUCTION TO THE INVENTION

In recent years, the amount of content protection systems is growing in a rapid pace. Some of these systems only protect the content against illegal copying, while others are also prohibiting the user to get access to the content. The first category is called Copy Protection (CP) systems. CP systems have traditionally been the main focus for consumer electronics (CE) devices, as this type of content protection is thought to be cheaply implemented and does not need bi-directional interaction with the content provider. Some examples are the Content Scrambling System (CSS), the protection system of DVD ROM discs and DTCP, the protection system for IEEE 1394 connections.

The second category is known under several names. In the broadcast world, systems of this category are generally known as conditional access (CA) systems, while in the Internet world they are generally known as Digital Rights Management (DRM) systems.

Some type of CP systems can also provide services to interfacing CA or DRM systems. Examples are the systems currently under development by the DVB-CPT subgroup and the TV-Anytime RMP group. The goal is a system in which a set of devices can authenticate each other through a bi-directional connection. Based on this authentication, the devices will trust each other and this will enable/allow them to exchange protected content. The accompanying licenses describe which rights the user has and what operations he is allowed to perform on the content. The license is protected by means of some general network secret, which is only exchanged between the devices within a certain household. This network of devices is called Authorized Domain (AD).

In some of the current proposals for authorized domains, the number of devices is the main limitation of the size of the authorized domain. The proposals (like the SmartRight system developed by Thomson Multimedia) have a fixed maximum of the number of devices that might be part of the authorized domain. The main reason for limiting the size of the domain is to prevent domains from spreading unbounded over the Internet, where people open their authorized domain for complete strangers at the other end of the world. By limiting the size of the authorized domain, people have the incentive to allow only their own devices to be part of the domain.

This fixed maximum on the number of devices in the authorized domain has a number of disadvantages. One disadvantage is the fact that when a device breaks down or gets stolen, it is difficult to recover the rights associated with this device in the authorized domain, because the admission of devices to the domain may not be centrally controlled and it is also not archived which particular devices are part of the domain at any time.

A further disadvantage of the fixed maximum is the fact that it is very difficult to determine beforehand what a reasonable value of the maximum is. Especially when in the future more networked devices are hooked up to the home network, the values that seem reasonable today may be far too low in the future. However, it is very complex to implement such a fixed maximum in a way that allows easy upgrading of the maximum in the future.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a system in which the size of a particular domain can be restricted, whilst overcoming the disadvantages associated with a fixed maximum on the number of the devices in the particular domain.

This object is achieved according to the present invention in a system in which the number of simultaneously active sessions is used as a measure or indication of the domain size. This number could be, for example, the number of content items accessed at the same time, or the number of activated rendering devices.

In one embodiment, devices need to register themselves at the authorized domain in the normal way, but the total number of devices that can register is unlimited. On top of this registration, a device needs to open a session to a security module, such as a smartcard. The total limitation of the network size is in this embodiment accomplished by limiting the number of security modules in cooperation with limiting the number of sessions that a security module supports. As will become apparent below, many alternative embodiments are possible within the scope of the invention.

One could for example use as security module a smart card that supports only one session (i.e. with the device that holds the smart card) and the total number of smart cards permitted to be used in the domain at one time is limited to a certain maximum.

Important in this implementation is to prevent "session-hopping". 'Session-hopping' is a possible mechanism to share sessions over the Internet. People who have spare (unused) sessions in their own domain, might want to share those sessions over the Internet, thereby escaping from the basic requirement set on authorized domains, i.e. limiting the distribution of content over the Internet. This issue can be addressed by installing

mechanisms as allowing a device to be registered at only one authorized domain and installing time delays that limit changing the registration to for instance once per day. This could be replaced with or combined with requiring an active action of the domain holder, possibly a physical action on one of the domain devices.

BRIEF DESCRIPTION OF THE FIGURES

These and other aspects of the invention will be apparent from and elucidated with reference to the illustrative embodiments shown in the drawings, in which:

Fig. 1 schematically shows a system comprising devices interconnected via a network;

Fig. 2 schematically shows the schematic division of the system 100 of Fig. 1 into a CA domain and a CP domain; and

Fig. 3 schematically shows a preferred embodiment of a security module, in the form of a smart card, for use in the system of Fig. 1.

Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

SYSTEM ARCHITECTURE

Fig. 1 schematically shows a system 100 comprising devices 101-105 interconnected via a network 110. In this embodiment, the system 100 is an in-home network. A typical digital home network includes a number of devices, e.g. a radio receiver, a tuner/decoder, a CD player, a pair of speakers, a television, a VCR, a tape deck, and so on. These devices are usually interconnected to allow one device, e.g. the television, to control another, e.g. the VCR. One device, such as e.g. the tuner/decoder or a set top box (STB), is usually the central device, providing central control over the others.

Content, which typically comprises things like music, songs, movies, TV programs, pictures, books and the likes, but which also includes interactive services, is received through a residential gateway or set top box 101. The source could be a connection to a broadband cable network, an Internet connection, a satellite downlink and so on. The content can then be transferred over the network 110 to a sink for rendering. A sink can be, for instance, the television display 102, the portable display device 103, the mobile phone 104 and/or the audio playback device 105.

The exact way in which a content item is rendered depends on the type of device and the type of content. For instance, in a radio receiver, rendering comprises generating audio signals and feeding them to loudspeakers. For a television receiver, rendering generally comprises generating audio and video signals and feeding those to a display screen and loudspeakers. For other types of content a similar appropriate action must be taken. Rendering may also include operations such as decrypting or descrambling a received signal, synchronizing audio and video signals and so on.

The set top box 101, or any other device in the system 100, may comprise a storage medium S1 such as a suitably large hard disk, allowing the recording and later playback of received content. The storage medium S1 could be a Personal Digital Recorder (PDR) of some kind, for example a DVD+RW recorder, to which the set top box 101 is connected. Content can also be enter the system 100 stored on a carrier 120 such as a Compact Disc (CD) or Digital Versatile Disc (DVD).

The portable display device 103 and the mobile phone 104 are connected wirelessly to the network 110 using a base station 111, for example using Bluetooth or IEEE 802.11b. The other devices are connected using a conventional wired connection. To allow the devices 101-105 to interact, several interoperability standards are available, which allow different devices to exchange messages and information and to control each other. One well-known standard is the Home Audio/Video Interoperability (HAVi) standard, version 1.0 of which was published in January 2000, and which is available on the Internet at the address http://www.havi.org/. Other well-known standards are the domestic digital bus (D2B) standard, a communications protocol described in IEC 1030 and Universal Plug and Play (http://www.upnp.org).

It is often important to ensure that the devices 101-105 in the home network do not make unauthorized copies of the content. To do this, a security framework, typically referred to as a Digital Rights Management (DRM) system is necessary.

In one such framework, the home network is divided conceptually in a conditional access (CA) domain and a copy protection (CP) domain. Typically, the sink is located in the CP domain. This ensures that when content is provided to the sink, no unauthorized copies of the content can be made because of the copy protection scheme in place in the CP domain. Devices in the CP domain may comprise a storage medium to make temporary copies, but such copies may not be exported from the CP domain. This framework is described in European patent application 01204668.6 (attorney docket PHNL010880) by the same applicant as the present application.

Regardless of the specific approach chosen, all devices in the in-home network that implement the security framework do so in accordance with the implementation requirements. Using this framework, these devices can authenticate each other and distribute content securely. Access to the content is managed by the security system. This prevents the unprotected content from leaking to unauthorized devices and data originating from untrusted devices from entering the system.

Fig. 2 schematically shows the schematic division of the system 100 of Fig. 1 into a CA domain and a CP domain. In Fig. 2, the system 100 comprises a source, a sink, and two storage media S1 and S2. Most content enters the in-home network in the CA domain through the set-top box 101 (the source). Typically, the sinks, for instance the television system 102 and the audio playback device 105, are located in the CP domain. This ensures that when content is provided to the sink, no unauthorized copies of the content can be made because of the copy protection scheme in place in the CP domain.

A CA→CP gateway is provided between the CA and the CP domains. This gateway is responsible for letting content enter the CP domain. This process may require transcoding and/or (re-)encrypting the content, translating digital rights associated with the content to a format supported in the CP domain, and so on.

The CP domain comprises a storage medium S2, on which (temporary) copies of the content can be stored in accordance with the copy protection rules. These copies can be used for time-shifted playback of the content, but these copies may not be exported from the CP domain.

A device becomes part of the CP domain by connecting it to another device already in the CP domain, or by connecting it to the bus connecting these devices. Once a device has been added, it must remain in that particular CP domain for a certain period of time, for example one day.

SECURITY MODULES

Fig. 3 schematically shows a preferred embodiment of a security module, shown here in the form of a smart card 300. To protect content against unauthorized copying, instances of content are provided to the system 100 in encrypted form. Before it can be rendered it needs to be decrypted, using a control word. Handling control words and/or decrypting instances of content is the responsibility of the security module. The security module should therefore be well protected against tampering.

Of course there are many ways to implement security modules. A common secure solution is to embody the security module in the form of a smart card. The security module could also be provided as an integrated component of one of the devices 101-105, or as a separate device. The security module can be embodied in hardware, software or a combination thereof.

The smart card 300 comprises a conditional access module 310 and a secure storage module 311. Smart cards are much more difficult to compromise than ordinary computers or software and so offer a better way of protecting the conditional aspects of a conditional access service. One or more of the devices 101-105 is then equipped with a smart card reader, in which the user can insert the smart card 300.

The control word necessary to decrypt the content can be stored in the secure storage module 301 on the smart card 300. This way, it is very difficult for the user to obtain the control word, and so it is very difficult for him to access the content without paying for it. The smart card 300 may comprise a decryption module 312, which decrypts an instance of the content using the control word and supplies the decrypted instance to a rendering device such as television 102.

Alternatively, the smart card 300 can supply the control word to another device which then decrypts the instance. In this case, there is the risk that this other device has been tampered with in such a way that it will not simply decrypt the content, but instead store the control word or store the unencrypted content without authorization to do so. In order to prevent such a modified device from accessing the control word, the smart card 300 may employ an authentication mechanism in order to verify whether the device has been tampered with.

This authentication mechanism is for instance realized by having the smart card issue an encrypted 'challenge' to the device, which the device must decrypt and send back to the smart card 300. If the device cannot correctly decrypt the challenge, it is not a compliant device and may not get access to the control word. Alternatively, the smart card 300 can check the integrity of some part of the program code to be executed by the device, for example by verifying a digital signature.

The control word may be provided in an Entitlement Control Message (ECM) that is sent to the system 100 by the service provider providing the encrypted service. It could also be stored permanently in the smart card 300. This ECM is then provided to the smart card 300 and thereby to the conditional access module 310, which obtains the control word from the ECM. The control word will often be present in an encrypted form in the ECM, and

so the conditional access module 310 will need to decrypt the control word first. The decryption key necessary to decrypt the control word can then be stored in the secure storage module 311.

In accordance with the present invention, the smart card 300 is also provided with a session management module 313. The term "session" refers to the handling of a specific instance of a content item, in particular decrypting the instance and supplying the decrypted instance to the rendering device. Handling may be restricted to a portion of the instance (e.g. the audio channels or the video stream of a movie), or cover the instance as a whole (audio, video, Teletext information, and so on). Another definition of a "session" could be the number of active devices, or the number of active "display" devices (e.g. TV, monitor, audio amplifier, ...). The smart card 300 is a central entity in this process.

It may be that two rendering devices are simultaneously rendering the same television program, or that one rendering device is playing back a piece of music and a storage device is making a copy of the same piece of music at the same time. In both cases the system 100 is handling two simultaneous sessions, even if both devices are operating on the same stream of data.

SESSION RESTRICTION

The session management module 313 is operable to restrict the number of simultaneous sessions that the smart card 300 is permitted to handle. This way, the owner of the system 100 can connect an unlimited number of devices to the system 100, but he will not be able to view or listen to many instances of content at the same time. If the entire system 100 is located within one household, this is not a problem, assuming a reasonable upper limit on the number of simultaneous sessions is chosen.

If the devices in the system 100 are distributed over various houses in a particular district, the same upper limit seriously restricts the use of the devices. For example, if the upper limit is set to twelve simultaneous sessions, all members of an average household should [illegible] favorite television programs, listen to the radio and at the same time record their favorite movie on another channel. However, if [illegible]